Theoretical Computer Science 116 (1993) 415–419
Elsevier

Note

On shifting networks

Pavel Pudlák

Mathematical Institute, ČSAV, Žitná 25, Praha 1, Czech Republic

Petr Savický

Department of Logic, Faculty of Philosophy, Charles University, Náměstí J. Palacha 2, Praha 1, Czech Republic

Communicated by M.S. Paterson
Received January 1991
Revised April 1992

Abstract

Pudlák, P. and P. Savický, On shifting networks, Theoretical Computer Science 116 (1993) 415–419.

We show nonlinear lower bounds on boolean circuits of depth 2, with arbitrary boolean functions and unbounded fan-in, which compute shifts. We give an explicit construction of a certain network related to the above circuits.

We consider the problem of proving the lower bounds on the size of circuits that compute shifts. Let x and y be nonnegative integers, we assume that they are given in binary. The shift operation is the binary operation $x \cdot 2^y$. We shall assume that the length of x is n and the length of y is $\lceil \log_2 n \rceil$. Furthermore, we are interested only in the processing of x; this can be formalized e.g. by assuming that any function depending only on y is given for free. We shall use an equivalent way of formalizing this, which is to consider only x as the input and allow the gates to be adjusted for each y.

We shall consider circuits of bounded depth with arbitrary fan-in and which can use arbitrary boolean functions as gates. We shall prove nonlinear lower bounds on the

Correspondence to: P. Pudlák, Mathematical Institute, ČSAV, Žitná 25, Praha 1, Czech Republic.

size (=the number of edges) of such circuits computing shifts. The proof is based on defining a graph property, called *interval shifters*, weaker than the property of being a superconcentrator. An easy argument shows that each circuit computing shifts is an interval shifter. Then we prove the lower bounds by modifying the proof for superconcentrators of Pippenger [2]. We also present a simple explicit construction of interval shifters.

As the shift operation is implicit in multiplication, such bounds are also lower bounds on the size of multiplication circuits. However, the lower bounds for multiplication that can be derived from our lower bounds for circuits that compute shifts can also be derived from the lower bounds for weak superconcentrators proved in [1].

1. Definitions

Let G be a directed acyclic graph with n inputs $x_0, \ldots, x_{n-1}$, and n outputs $y_0, \ldots, y_{n-1}$.

(1) G is called a *shifter* if, for every shift s, there are vertex disjoint paths from x_i to $y_{i+s(\mathrm{mod}\, n)}$, for $i=0, \ldots, n-1$.

(2) G is called a *boolean shifter* if, for every shift s, one can assign boolean functions to the vertices so that it computes the shift s, i.e. $y_i = x_{i+s(\mathrm{mod}\, n)}$, for $i=0, \ldots, n-1$.

(3) G is called *an interval shifter* if, for every interval $I \subseteq [0, n-1]$ and every shift s, there are vertex-disjoint paths connecting the vertices x_i, $i \in I$, with the vertices of y_j, $j \in I+s(\mathrm{mod}\, n)$. (We consider intervals on the cycle; thus, e.g. I can be $\{i, i+1, \ldots, n-1, 0, 1, \ldots, j\}$.)

(4) G is called a *set distributor* if, for every $k=1, \ldots, n$, there are n subsets of inputs and n subsets of outputs each of cardinality k such that each input vertex is in exactly k subsets and each output vertex is in exactly k subsets and each of the subsets of inputs is connected with each of the subsets of outputs by k vertex disjoint paths.

(5) G is called a *superconcentrator* if, for all pairs $A, B \subseteq [0, n-1]$ of subsets of equal cardinality, there are vertex-disjoint paths connecting the vertices x_i, $i \in A$, with the vertices of y_j, $j \in B$.

Note that in (3)–(5) we do not require paths between particular pairs of vertices, we only require that each vertex in one set is connected with some vertex in the other set.

We are interested in the minimal size of boolean shifters. (The difference between cyclic and ordinary shifts is inessential.) While the asymptotic behaviour of the minimal size of shifters has been determined [5], this is an open problem for boolean shifters. Our tool will be interval shifters. Distributors are introduced only in order to have as weak assumptions as possible in the following theorem.

2. Results

Lemma 2.1. *The dependence between the concepts defined above is:*

$$(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (4) \quad \text{and} \quad (5) \Rightarrow (3).$$

Proof. (1) $\Rightarrow$ (2): Use projection functions.
(2) $\Rightarrow$ (3): By a standard information-theoretic argument.
(3) $\Rightarrow$ (4) and (5) $\Rightarrow$ (3): Trivially by definition. □

Theorem 2.2. *The number of edges in a set distributor of depth* 2 *is* $\Omega(n \log n)$.

Proof. The proof of the lower bound for superconcentrators of [2] can be carried out with a slight modification.

Let a set distributor of depth 2 be given. Let $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_n\}$. In order to simplify the computations, we shall assume, moreover, that $n = 2^k$. Let V denote the set of vertices on the middle level; for $v \in V$, denote by f_v (g_v) the in-degree (out-degree) of v. Let i, $1 \leqslant i \leqslant k$, be given. Take randomly and independently sets $A \subseteq X$ and $B \subseteq Y$ of size 2^{k-i} given by the definition of the set distributor. Then, for $x \in X$ (for $y \in Y$) the probability that $x \in A$ ($y \in B$) is 2^{-i}. Thus, the probability that v is connected with A and B is at most

$$f_v \cdot 2^{-i} \cdot g_v \cdot 2^{-i} \leqslant (f_v + g_v)^2 \cdot 2^{-2i-2},$$

and is, of course, at most 1. This estimate was established in [2] in a different way. The rest of the proof follows the proof of [2]. Since we assume that there are 2^{k-i} disjoint paths connecting A and B, the mean value of the number of vertices in V connected with A and B must be at least this number. Thus, we get the following inequality:

$$\sum_{v \in V} \min((f_v + g_v)^2 \cdot 2^{-2i-2}, 1) \geqslant 2^{k-i}.$$

Hence,

$$\sum_{v \in V} \min((f_v + g_v)^2 \cdot 2^{-i-2}, 2^i) \geqslant 2^k.$$

Summing over i and interchanging the summations, we have

$$\sum_{v \in V} \sum_{i} \min((f_v + g_v)^2 \cdot 2^{-i-2}, 2^i) \geqslant k \cdot 2^k.$$

The inner sum will now be split according to which of the terms are minimal:

$$\sum_{f_v + g_v < 2^{i+1}} (f_v + g_v)^2 \cdot 2^{-i-2} + \sum_{f_v + g_v \geqslant 2^{i+1}} 2^i \leqslant (f_v + g_v)^2 \cdot \frac{1}{(f_v + g_v)} + (f_v + g_v)$$
$$\leqslant 2(f_v + g_v).$$

Thus,

$$\sum_{v \in V} 2(f_v + g_v) \geqslant k \cdot 2^k \Rightarrow \sum_{v \in V} (f_v + g_v) \geqslant k \cdot 2^{k-1}. \qquad \square$$

Corollary 2.3. *There are no boolean shifters of depth 2 and linear size.*

However, there remains a big gap between upper bounds and lower bounds on the size of boolean shifters. The best upper bound that we know of follows from an easy bound $O(n^{1+1/d})$ for depth-d shifter graphs. We shall now describe a simple construction of a depth-2 interval shifter of size $O(n \cdot \log n)$.

Proposition 2.4. *There is a simple explicit construction of an interval shifter of depth 2 and size* $O(n \cdot \log n)$.

Proof. It is sufficient to construct interval shifters for $n = 2^k$, since the others can be obtained from these by "wrapping around". For $n = 2^k$, the proposition follows immediately from the next lemma.

Lemma 2.5. *There is a simple explicit construction of a bipartite graph* $E \subseteq X \times Y$, $|X| = 2^k$, $|Y| = 2^{k+1} - 1$, $|E| = (k+1)2^k$, *such that, for any* $d \leqslant 2^k$, *there exists a set* Y_d *such that, for every interval* $I \subseteq X$ *of length* d, *there is a matching between* I *and* Y_d *contained in* E.

Proof. Let $X = [0, 2^k - 1]$, $Y = \{v \in \{0,1\}^* \mid |v| \leqslant k\}$. Define E by

$$(u, v) \in E \equiv_{\text{def}} v \text{ is an initial segment of the binary expansion of } u.$$

For instance, the empty sequence Λ is connected with all $u \in X$. Clearly, $|E| = (k+1)2^k$. Now, let $d \leqslant 2^k$. Represent d as

$$d = 2^{i_1} + \cdots + 2^{i_m}, \quad i_1 < \cdots < i_m.$$

Then take

$$Y_d = \{v \in Y \mid |v| \in \{i_1, \ldots, i_m\}\}.$$

Let $I = [a, a+d-1]$ be an interval of length d. Take the following partition of I:

$$[a, a+d-1] = [a, a+2^{i_1} - 1] \cup [a+2^{i_1}, a+2^{i_1} + 2^{i_2} - 1]$$
$$\cup \cdots \cup [a+2^{i_1} + \cdots + 2^{i_{m-1}}, a+2^{i_1} + \cdots + 2^{i_m} - 1].$$

Each interval $[a+2^{i_1} + \cdots + 2^{i_{j-1}}, a+2^{i_1} + \cdots + 2^{i_j} - 1]$ has a matching with the subset $\{v \in Y \mid |v| = i_{j+1}\}$ of Y_d, and these subsets form a partition of Y_d. Thus, there is a matching between I and Y_d. $\square$

The lower bound can be extended to all depths; namely, for each fixed depth there is a nonlinear lower bound for boolean shifters. A general theorem which implies this will be published in a forthcoming paper [6].

References

[1] D. Dolev, C. Dwork, N. Pippenger, A. Widgerson, Superconcentrators, generalizers and generalized connectors with limited depth, in: *Proc. 15th Ann. ACM Symp. on Theory of Computing* (1983) 42–51.
[2] N. Pippenger, Superconcentrators of depth 2, *J. Comput. System Sci.* **24** (1982) 82–90.
[3] N. Pippenger, Communication networks, in: J. van Leeuwen, ed., *Handbook of Theoretical Computer Science, Vol. A* (Elsevier, Amsterdam, 1990) 805–833.
[4] N. Pippenger and L. Valiant, Shifting graphs and their applications, *J. ACM* **23** (1976) 423–432.
[5] N. Pippenger and A.C.-C. Yao, Rearrangable networks with limited depth, *SIAM J. Algebraic Discrete Methods* **3** (1982) 411–417.
[6] P. Pudlák, Communication in bounded depth circuits, *Combinatorica*, to appear.